UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/769,104	01/30/2004	Catalin D. Sandu	MSFT122167	9006

26389 7590 12/27/2007

CHRISTENSEN, O'CONNOR, JOHNSON, KINDNESS, PLLC
1420 FIFTH AVENUE
SUITE 2800
SEATTLE, WA 98101-2347

EXAMINER	
HAILU, TESHOME	
ART UNIT	**PAPER NUMBER**
2139	
MAIL DATE	**DELIVERY MODE**
12/27/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/769,104	SANDU ET AL.	
	Examiner	Art Unit	
	Teshome Hailu	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 October 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 January 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in reply to an amendment filed on October 10, 2007. Claims 1-5 have been amended.

2. Claims 6-20 have been added.

3. Claims 1-20 are pending.

Response to Amendment

4. Applicant's arguments with respect to claims 1-5 have been considered but are moot in view of the new ground(s) of rejection.

Applicant's arguments filed on October 10, 2007, with respect to 35 U.S.C. 101 rejections of claims 1-5 have been fully considered in view of the amendment to the claims and are persuasive. The 35 U. S. C. 101 rejections of claims 1-5 has been withdrawn.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hayashi et al (Hayashi), US 7,167,988, and further in view of HO, US 7,188,369

As Per claim 1 Hayashi discloses:

A normalization module that obtains an executable script, and generates a normalized signature for the executable script: wherein generating a normalized signature for the executable script comprises translating tokens from the executable script into normalized tokens conforming to a common format; (column 8, line 1-9, the normalization code stream outputted from the normalization processing unit is input to signature processing unit for generating normalization signature).

Wherein the malware detection system is configured to: compare the normalized signature of the executable script to the at least one normalized malware signature in the malware signature store to determine whether the executable script is malware; and report whether the executable script is malware according to the determination. (Abstract, line 10-16, compares the first hash value and the second hash value and judges the code stream is (is not) falsified).

A computer-implemented malware detection system for determining whether an executable script is malware according to its functionality, the malware detection system comprising: A malware signature store including at least one known malware script signature, wherein each malware signature in the malware signature store is a normalized signature of a known malware script; (column 8, line 1-9, the signature processing unit 13 generates signature data for the inputted normalization code stream).

Hayashi does not explicitly discloses, malware signature store. However, on the same field of endeavor, Ho teaches this limitation as, (abstract, line 1-6, an antivirus database comprising a plurality of computer virus signatures for detecting a malware).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Hayashi and include the above limitation using the teaching of Ho. The modification would be obvious because one of ordinary skill in the art would be motivated to add the above limitation for enhancing the security of the system by providing an antivirus system (column 1, line 50-55).

As per claim 2 Hayashi discloses:

The malware detection system of Claim 1, further comprising a comparison module, wherein the comparison module compares the normalized signature of the executable script to the at least one normalized signature in the malware signature store for the malware detection system. (Abstract, line 10-16, compares the first hash value of normalized code stream and the second hash value and judges the code stream is (is not) falsified).

As per claims 3, 4 and 5 Hayashi discloses:

A normalization means that obtains an executable script, and generates a normalized signature for the executable script, wherein the normalized signature for the executable script comprises a set of normalized tokens translated from corresponding tokens in the executable script into a common format suitable for comparison with the at least one malware signature in the malware signature store means, (column 8, line 1-9, the normalization code stream outputted from the normalization processing unit is input to signature processing unit for generating normalization signature).

A comparison means that compares the normalized signature for the executable script to the at least one malware signature in the malware signature storage means; wherein the malware detection system is configured to determine whether the executable script is malware according to the comparison performed by the comparison means, and report whether the executable script is malware. (Abstract, line 10-16, compares the first hash value and the second hash value of normalized code stream and judges the code stream is (is not) falsified).

A computer-implemented malware detection system for determining whether an executable script is malware the malware detection system comprising: a malware signature storage means including at least one known malware signature, wherein each malware signature in the malware signature store means is a normalized signature of a known malware script; (column 8, line 1-9, the signature processing unit 13 generates signature data for the inputted normalization code stream).

Hayashi does not explicitly discloses, malware signature store. However, on the same field of endeavor, Ho teaches this limitation as, (abstract, line 1-6, an antivirus database comprising a plurality of computer virus signatures for detecting a malware).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Hayashi and include the above limitation using the teaching of Ho. The modification would be obvious because one of ordinary skill in the art would be motivated to add the above limitation for enhancing the security of the system by providing an antivirus system (column 1, line 50-55).

As per claim 6 Hayashi discloses:

The malware detection system of Claim 2, wherein translating tokens from the executable script into a common format suitable for comparison with the at least one malware signature in the malware signature store comprises renaming tokens from the executable script according to a common naming convention. (Column 11, line 8-15, the normalization processing unit applies the normalization process to the code stream).

Hayashi does not explicitly discloses, malware signature in malware signature store. However, on the same field of endeavor, Ho teaches this limitation as, (abstract, line 1-6, an antivirus database comprising a plurality of computer virus signatures for detecting a malware).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Hayashi and include the above limitation using the teaching of Ho. The modification would be obvious because one of ordinary skill in the art would be motivated to add the above limitation for enhancing the security by providing an antivirus system (column 1, line 50-55).

As per claim 10 Hayashi discloses:

The malware detection system of Claim 3, wherein determining whether the executable script is

malware according to the comparison performed by the comparison means comprises determining whether the comparison found a complete match between the normalized signature for the executable script and a normalized malware signature in the malware signature store means and if so, reporting that the executable script is malware. (Column 11, line 8-15, the normalization processing unit applies the normalization process to the code stream).

Hayashi does not explicitly discloses, malware signature in malware signature store. However, on the same field of endeavor, Ho teaches this limitation as, (abstract, line 1-6, an antivirus database comprising a plurality of computer virus signatures for detecting a malware).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Hayashi and include the above limitation using the teaching of Ho. The modification would be obvious because one of ordinary skill in the art would be motivated to add the above limitation for enhancing the security by providing an antivirus system (column 1, line 50-55).

As per claims 13 and 17 Hayashi discloses:

The method of Claim 4, wherein determining, based on the previous comparison, whether the executable script is malware comprises determining if the first normalized signature for the executable script is a complete match with a normalized signature of known malware, and if so, reporting that the executable script is malware. (Column 11, line 8-15, the normalization processing unit applies the normalization process to the code stream).

Hayashi does not explicitly discloses, malware signature in malware signature store. However, on the same field of endeavor, Ho teaches this limitation as, (abstract, line 1-6, an antivirus database comprising a plurality of computer virus signatures for detecting a malware).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Hayashi and include the above limitation using the teaching of Ho. The modification would be obvious because one of ordinary skill in the art would be

motivated to add the above limitation for enhancing the security by providing an antivirus system (column 1, line 50-55).

As per claims 7, 11, 14, 16, and 18 Hayashi discloses:

The malware detection system of Claim 6 further configured to: if the prior determination indicates that the executable script is a partial match to at least one malware signature in the malware signature store: generate a second normalized signature for the executable script, wherein generating a second normalized signature comprises translating tokens from the executable script into a second common format suitable for comparison with a second normalized malware signature of known malware in the malware signature store; (column 8, line 1-9, the normalization code stream outputted from the normalization processing unit is input to signature processing unit for generating normalization signature).

Determine whether the executable script is malware according to a comparison between the second normalized signature and at least one second normalized signature in the malware signature store. (Column 8, line 1-9, the signature processing unit 13 generates signature data for the inputted normalization code stream).

Hayashi does not explicitly discloses, malware signature store. However, on the same field of endeavor, Ho teaches this limitation as, (abstract, line 1-6, an antivirus database comprising a plurality of computer virus signatures for detecting a malware).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Hayashi and include the above limitation using the teaching of Ho. The modification would be obvious because one of ordinary skill in the art would be motivated to add the above limitation for enhancing the security of the system by providing an antivirus system (column 1, line 50-55).

As per claims 8, 12, 15 and 19 Hayashi discloses:

The malware detection system of Claim 7, wherein translating tokens from the executable script into a second common format suitable for comparison with a second normalized malware signature of known malware in the malware signature store comprises translating tokens of the executable script into a common name according to each token's type. (Column 11, line 8-15, the normalization processing unit applies the normalization process to the code stream).

Hayashi does not explicitly discloses, malware signature in malware signature store. However, on the same field of endeavor, Ho teaches this limitation as, (abstract, line 1-6, an antivirus database comprising a plurality of computer virus signatures for detecting a malware).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Hayashi and include the above limitation using the teaching of Ho. The modification would be obvious because one of ordinary skill in the art would be motivated to add the above limitation for enhancing the security by providing an antivirus system (column 1, line 50-55).

As per claim 9 Hayashi discloses:

The malware detection system of Claim6, wherein generating a normalized signature for the executable script further comprises generating a set of normalized tokens for each routine in the executable script. (Column 7, line 27-35, several parameters are designated in normalization method. For example, in the case of an image coding system described later, the number of divisions of discrete wavelet conversion, a type of a progressive order, presence or absence of execution of arithmetic coding of a lower bit plane, a size of a code block, and the like are designated).

As per claim 20 Hayashi discloses:

The computer-readable medium of Claim 19, wherein the method further comprises comparing the second normalized signature for the executable script to second normalized signatures of known malware to determine whether the second normalized signature for the executable script is a partial

match to a second normalized signature of known malware, and if so, reporting that the executable script is potential malware. (Column 11, line 8-15, the normalization processing unit applies the normalization process to the code stream).

Hayashi does not explicitly discloses, malware signature in malware signature store. However, on the same field of endeavor, Ho teaches this limitation as, (abstract, line 1-6, an antivirus database comprising a plurality of computer virus signatures for detecting a malware).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Hayashi and include the above limitation using the teaching of Ho. The modification would be obvious because one of ordinary skill in the art would be motivated to add the above limitation for enhancing the security by providing an antivirus system (column 1, line 50-55).

Conclusion

7. The prior art made or record and not relied upon is considered pertinent to applicant's disclosure.

TITLE: Detection of polymorphic script language viruses by data driven lexical analysis, US Pub. No. 2002/0073330.

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Teshome Hailu whose telephone number is (571) 270-3159. The examiner can normally be reached on Mon-Fri 7:30a.m. to 5:00p.m. PST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Teshome Hailu

December 21, 2007

SYED A. ZIA 12/21/2007
PRIMARY EXAMINER